UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/740,843	12/21/2000	Takayuki Sugahara	0102/0151	6519

21395 7590 08/16/2004

LOUIS WOO
LAW OFFICE OF LOUIS WOO
717 NORTH FAYETTE STREET
ALEXANDRIA, VA 22314

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 08/16/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/740,843	SUGAHARA ET AL.	
	Examiner	Art Unit	
	Brandon Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *01 June 2004* .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *11-16 and 21-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *11-16 and 21-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 11-16 and 21-28 are pending in this office action, claims 7-10 and 17-20 are canceled.

2. Applicant's arguments filed June 1, 2004, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 102

Claims 14-16, and 25-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Pinder et al. (U.S. Patent No. 6,105,134).

Regarding claims 14 and 25, Pinder et al. teaches a method/apparatus of decrypting contents information, comprising the steps of:

- Receiving encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a transmission line (fig. 2B, TDS to DEMULTIPLEXER);
- Generating an authentication value from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been

generated by an encryption-resultant contents information provider side (fig. 2B, ref. num 232),

- The generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information (col. 7, lines 4-6);

- Generating second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function, the second-key base information being a base of a second key (fig. 2B, ref. num 234);
- Generating a second-key signal representative of the second key from the generated second-key base information according to a second function (fig. 2B, MSK);
- Decrypting the reproduced encryption-resultant first-key base information into recovered first-key base information in response to the generated second-key signal, the recovered first-key base information being a base of a first key (fig. 2B, ref. num 236);
- Generating a first-key signal representative of the first key from the recovered first key base information according to a third function (fig. 2B, CW); and
- Decrypting the reproduced encryption-resultant contents information in response to the generated first-key signal to recover original contents information (fig. 2B, ref. num 238).

Regarding claims 15 and 26, Pinder et al. teaches wherein the first function is inverse with respect to a function which has been used by the encryption-resultant contents information provider side to generate the transmission-purpose key base information (col. 8, lines 39-63).

Regarding claims 16 and 27, Pinder et al. teaches wherein the second and third functions are one-way functions (col. 8, line 64 through col. 9, line 24 and lines 41-55).

Regarding claim 28, Pinder et al. teaches further comprising means for allowing a user to input the issue ID information (col. 15, lines 36-55).

Claim Rejections - 35 USC § 103

4. Claims 11-13, and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder et al. (U.S. Patent No. 6,105,134).

Regarding claims 11 and 21, Pinder et al. teaches a method/apparatus of decrypting contents information, comprising the steps of:

- Receiving encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a transmission line (fig. 2B, TDS to DEMULTIPLEXER);
- Generating an authentication value from a decryption-side ID information peculiar to a decryption side and previously-fed issue ID information which has been

generated by an encryption-resultant contents information provider side (fig. 2B, ref. num 232),

- The generated authentication value is equal to an authentication value used to generate the transmission-purpose key base information (col. 7, lines 4-6);

- Generating second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function, the second-key base information being a base of a second key (fig. 2B, ref. num 234);
- Generating a second-key signal representative of the second key from the generated second-key base information according to a second function (fig. 2B, MSK);
- Decrypting the reproduced encryption-resultant first-key base information into recovered first-key base information in response to the generated second-key signal, the recovered first-key base information being a base of a first key (fig. 2B, ref. num 236);
- Generating a first-key signal representative of the first key from the recovered first key base information according to a third function (fig. 2B, CW); and
- Decrypting the reproduced encryption-resultant contents information in response to the generated first-key signal to recover original contents information (fig. 2B, ref. num 238).

Pinder et al. does not specifically teach reproducing encryption-resultant contents information, encryption-resultant first-key base information, and transmission-purpose key base information from a recording medium. However, the Examiner believes it to be well known to reproduce contents from a recording medium.

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to reproduce the contents data from a recording medium. It would have been obvious to one of ordinary skill in the art to reproduce the contents data from a recording medium because reproducing contents data from a recording medium allows the data to be saved prior to it use, therefore giving the user the freedom to choose when to use the data.

Regarding claims 12 and 22, Pinder et al. as modified teaches wherein the first function is inverse with respect to a function which has been used by the encryption-resultant contents information provider side to generate the transmission-purpose key base information (col. 8, lines 39-63).

Regarding claims 13 and 23, Pinder et al. as modified teaches wherein the second and third functions are one-way functions (col. 8, line 64 through col. 9, line 24 and lines 41-55).

Regarding claim 24, Pinder et al. teaches further comprising means for allowing a user to input the issue ID information (col. 15, lines 36-55).

Claims 24 and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Pinder et al. (U.S. Patent No. 6,105,134) in view of Widmer (U.S. Patent No. 4,313,031).

Regarding claims 24 and 28, Pinder et al. teaches all the limitations of claims 21 and 25, respectively, above. However, Pinder et al. does not teach further comprising means for allowing a user to input the issue ID information.

Widmer teaches further comprising means for allowing a user to input the issue ID information (fig. 1, ref. num 1).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine allowing a user to input the issue ID information, as taught by Widmer, with the apparatus of Pinder et al. It would have been obvious to one of ordinary skill in the art to combine allowing a user to input the issue ID information, as taught by Widmer, with the apparatus of Pinder et al. because an inputting means for the issue ID information would provide a way to encrypt/decrypt data directly based off of the data inputted from the input device instead of using predetermined keys. This allows the issue ID to be changed at anytime by the user of the system.

Response to Arguments

5. Applicant cancels claims 7-10 and 17-20.

6. Applicant argues:

a. Pinder et al. does not teach generating an authentication value from a decryption-side ID peculiar to a decryption side and previously-fed ID information which has been generated by an encryption-resultant contents information provider side (page 8, second paragraph).

b. There are contradictions about the first-key signal being generated from the recovered first-key base information according to the third function and the reproduced encryption-resultant contents information is decrypted in response to the generated first-key signal (page 9, second paragraph).

c. Pinder et al. does not teach generation of second-key base information from the reproduced transmission-purpose key base information and the generated authentication value according to a first function (page 10, third paragraph).

Regarding argument (a), examiner disagrees with applicant. As seen (col. 7, lines 6-9), the Public secure micro serial number selects an appropriate MSK addressed to the specific decoder. This is treated as a 'decryption-side ID information peculiar to a decryption side.' Also, as seen, (col. 6, lines 21-25), a symmetric algorithm is used for block 201, which provides 'previously-fed ID information which has been generated by an encryption-resultant contents information provider side.' A symmetric algorithm, by

nature, has to setup previously fed information to the receiver in order for proper decryption.

Regarding argument (b), examiner disagrees with applicant. Examiner points applicants to fig. 3 and col. 7, line 24 through col. 10, line 12 to provide a more clear representation of fig. 2A and 2B. The generation of first-key base information and second-key base information in application (fig. 1, ref. num 7 and 9) is synonymous with Pinder et al. (fig. 3, ref. num 339 and 343 and col. 8, lines 39-49 and col. 9, lines 41-55).

Regarding argument (c), examiner disagrees with applicant. The decrypter (fig. 2B, ref. num 234) is the part that 'generates' the second-key base information. By inputting the encrypted MSK and the private key, second-key base information is generated from a decryption process.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon Hoffman whose telephone number is 703-305-4662. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brandon Hoff

BH

E. Moise

EMMANUEL L. MOISE
PRIMARY EXAMINER
A/U 2136